Issue Brief

June 2025
No : 442

Operation ‘Spider’s Web’: Ukraine’s Evolution in Asymmetric Warfare

Brig Anubir Chahal (Retd)

Operation 'Spider's Web': Ukraine's Evolution In Asymmetric Warfare

Brig Anubir Singh Chahal (Retd)

Abstract

Operation Spider's Web exemplifies Ukraine's innovative use of AI-powered drones in asymmetric warfare, signalling a broader shift in modern conflict. The semi-autonomous attack, launched via modified trucks and operated through Russia's own telecom networks, demonstrates how agility and technological integration now rival industrial scale in determining battlefield outcomes. As unmanned systems become more accessible and effective, militaries must adapt through resilience, countermeasures, and doctrinal innovation to stay ahead in an evolving strategic landscape. This article will thoroughly analyse and de-construct operation Spider Web and Ukraine's Asymmetric capability

Keywords: Ukraine, Operation Spider's Web, AI drones, asymmetric warfare, unmanned systems,

Introduction

On June 1st, Ukraine's Security Service (SSU) launched what can only be described as one of the most daring and sophisticated drone operations of the war so far. Striking deep into Russian territory, the mission targeted four key air bases and dealt a heavy blow to Moscow's strategic bomber fleet. Aptly codenamed "Spider's Web" a reference to its wide and calculated reach across distant Russian locations previously believed to be out of Ukraine's range the operation demonstrated a remarkable leap in both ambition and capability (Bondar, 2025).

What made the strike particularly prominent, was its method. Small drones, discreetly transported into Russia inside hidden compartments of cargo trucks, were launched from within the country's own borders. These drones homed in on more than 40 high-value military aircraft, including Russia's prized Tu-95MS and Tu-22M3 bombers, as well as A-50 surveillance planes crucial tools used to coordinate missile attacks on Ukrainian cities.

Beyond the tactical success, the operation reflects a turning point in Ukraine's asymmetric warfare strategy. It reveals not just ingenuity and resolve, but also a deep vulnerability in Russia's rear defences, once considered safe, now proven to be exposed.

Key Targets

Operation *Spider's Web* focused on four strategically vital Russian military air bases, each integral to the functioning of the country's long-range aviation network. What made the operation especially significant was the geographic dispersion of these targets stretching across the full expanse of Russian territory. This broad and interconnected targeting approach likely inspired the operation's codename, evoking the image of a web cast wide across distant and seemingly secure locations.

.

Figure 01: Targeted Russian airbases During Ukrainian Drone Operation (Gibson et al., 2025)

Operation *Spider's Web* marked a significant evolution in Ukraine's asymmetric warfare strategy, targeting four of Russia's most strategically important air bases in a coordinated strike designed to disrupt the heart of its long-range strike and aerial surveillance capabilities. **The operation's codename evokes the image of a wide-reaching and intricately connected assault apt, given the geographical dispersion of the targets across Russia's vast expanse, from the Arctic Circle to Siberia.**

Olenya Air Base, situated in Murmansk Oblast on the Kola Peninsula—roughly 1,900 km north of Ukraine—houses the 40th Composite Aviation Regiment, including Tu-22M3 bombers. Its strategic importance increased after the redeployment of Tu-95MS bombers to this location, making it a critical hub for long-range missile launches. The belief that its remote Arctic location rendered it immune to Ukrainian strikes was definitively shattered.

Diaghilevo Air Base, in Ryazan Oblast, approximately 470 km from Ukraine, serves as Russia's central training and maintenance facility for strategic bomber crews and aircraft, including the Tu-95, Tu-160, and Tu-22M3 platforms. The attack on Diaghilevo not only

degraded Russia's current operational fleet but also disrupted critical support systems—training pipelines, maintenance cycles, and logistical throughput.

Belaya Air Base, in Irkutsk Oblast, more than 4,000 km from the Ukrainian border, had long been considered beyond the reach of Ukraine's strike capabilities. Hosting the 220th Heavy Bomber Aviation Regiment and their Tu-22M3 bombers equipped with Kh-22 cruise missiles, the strike on Belaya was the first confirmed Ukrainian attack on a deep Siberian target. It demonstrated not just technological advancement, but strategic signaling nowhere is beyond reach.

Ivanovo Air Base, located about 700 km from the border, is home to Russia's scarce fleet of A-50 AWACS aircraft crucial for airspace surveillance, threat detection, and command coordination. With Russia believed to possess fewer than ten such platforms, any losses here dramatically impair its air command-and-control infrastructure and situational awareness.

Although Russian authorities also reported attempted strikes in Amur Oblast, no confirmed damage has been verified.

In contextual terms, *Spider's Web* represents more than a tactical victory, it is a strategic message. It signals Ukraine's growing ability to conduct precision strikes at extended ranges, undermining Russia's assumptions about strategic depth and sanctuary. The operation exposed the fragility of Russia's rear-area defenses and demonstrated that Ukrainian forces can now threaten high-value targets previously considered untouchable. It also aligns with broader patterns of 21st-century warfare, where technologically adaptive actors leverage innovation, agility, and precision to offset conventional military asymmetries(Starchak, 2025)

Aviation Assets Destroyed

During Ukraine's *Spider's Web* operation, conducted by the Security Service of Ukraine (SSU), over 40 Russian military aircraft were confirmed destroyed or critically damaged across four key air bases. These losses represent a significant degradation of Russia's long-range strike and command capabilities. Notably, the aircraft affected include core platforms central to Russia's strategic bombing fleet and airborne battle management infrastructure (Borsari, 2025).

Among the aircraft targeted was the **Tu-95**, a Cold War-era strategic bomber powered by turboprop engines. Despite its vintage design, the Tu-95 remains an integral part of Russia's long-range strike arsenal, capable of deploying up to 16 cruise missiles—including the Kh-55, Kh-555, and the modern Kh-101/102. These platforms serve as primary delivery systems for both conventional and nuclear payloads.

The **Tu-22M3**, a supersonic long-range bomber, was also among the damaged assets. It is equipped to carry Kh-22 cruise missiles, which present a serious challenge to Ukrainian air defense systems due to their high velocity and low-altitude penetration profile. This aircraft remains a crucial component of both Russia's conventional and nuclear strike forces.

Another critical loss was the **A-50**, an Airborne Warning and Control System (AWACS) aircraft. Designed for airspace surveillance, target acquisition, and coordination of fighter and missile strikes, the A-50 provides command-and-control functions vital to Russia's battlefield awareness. With fewer than ten operational units in service and each valued at approximately $350 million, any attrition of this fleet substantially reduces Russia's operational intelligence and command cohesion.

Also affected was the **Tu-160**, the largest and most advanced combat aircraft in the Russian arsenal. This supersonic, variable-sweep wing strategic bomber is capable of delivering both conventional and nuclear munitions—including Kh-101 and Kh-102 cruise missiles. As a pillar of Russia's nuclear triad, the Tu-160's vulnerability signals broader implications for the credibility of its long-range deterrent posture.

Collectively, the aircraft impacted in this operation represent the technological backbone of Russia's ability to conduct strategic bombing and coordinate complex air operations. Their loss not only weakens immediate offensive potential but also imposes long-term setbacks on Russian airpower regeneration and deterrence capabilities (Borsari, 2025).

How the Operation Was Carried Out

Planning for Operation Spider's Web started more than 18 months before it happened. Ukrainian teams secretly moved about 150 small drones, launch equipment, and 300 explosive charges into Russia using hidden supply routes. The drones were packed inside wooden cabins that looked ordinary and were loaded onto regular cargo trucks.

A major part of the plan involved secretly moving equipment through Russia without raising suspicion. To do this, Ukraine's security service (SSU) is said to have hired Russian truck drivers who didn't know what they were carrying. These drivers were told exactly where and when to go and were asked to park near important Russian air bases—often at gas stations or on quiet roads.

At the right moment, the cabins' roofs were opened by remote control, and the drones took off directly from the trucks. This allowed the drones to fly short distances to their targets, avoiding Russia's air defence systems before they had time to respond. Russian reports confirmed that drones were launched from areas just outside the air bases. After launching the drones, the trucks exploded, showing they had been set up to destroy themselves.

Altogether, 117 drones were launched, and over 40 Russian aircraft were hit. Ukrainian sources say this damaged around 34% of Russia's aircraft that can launch cruise missiles. Among the targets were rare A-50 planes that help Russia watch the skies and guide its air operations.

All Ukrainian personnel involved left Russian territory safely before the drones were launched. The operation was closely managed by Ukrainian leaders, including President Zelensky and SSU chief Vasyl Maliuk.

The success of this mission showed that Ukraine can now carry out well-organized and far-reaching attacks inside enemy territory using its own technology and clever tactics that combine surprise, disguise, and precision.

AI's Role in Ukraine's "Spider's Web" Drone Operation

Operation Spider's Web showcased Ukraine's innovative use of drone warfare, blending human-operated systems with elements of autonomy and possible AI-enhanced functions. Although the drones were not fully autonomous, evidence indicates that artificial intelligence likely supported both flight control and targeting accuracy particularly in hitting vulnerable components of strategic aircraft(Bego, 2025).

The FPV (first-person-view) drones used in the operation were remotely piloted via Russian mobile telecom infrastructure, including 4G and LTE networks. These connections offered enough bandwidth to enable real-time video and command transmission over large distances, allowing Ukrainian forces to control the drones from outside Russian borders eliminating the need for nearby operators or ground control stations.

To maintain stable, long-distance control over these networks, the drones used a combination of software and hardware centered around ArduPilot an open-source autopilot system widely adopted for UAVs. ArduPilot supports advanced flight stabilization, automated routing, safety features, and programmable missions. In this operation, drones were equipped with compact computers (such as Raspberry Pi), webcams, and LTE modems connected through Ethernet. Video feeds guided the operators visually, while control signals passed through ArduPilot's UART interface, enabling steady and responsive piloting even under high-latency conditions.

ArduPilot's adaptive architecture made it particularly suitable for internet-based FPV missions operating under unstable links, as it could autonomously manage orientation, altitude, and direction while awaiting remote inputs. This capability proved critical for launching drones from makeshift platforms deep inside Russian territory.

Beyond manual piloting, there are indications that the drones employed AI-assisted targeting mechanisms. Open-source intelligence reports suggest that Ukrainian SSU teams analyzed the design and visual signatures of aircraft such as the Tu-95MS, Tu-22M3, and A-50—many of which are on display in aviation museums like the one in Poltava to pinpoint structural vulnerabilities.

These assessments likely helped develop machine vision models trained to recognize key weak spots, such as underwing missile mounts and fuel seam lines. These models, embedded into the drones' onboard systems, could assist operators in identifying targets and executing precise terminal attacks. Visual evidence released by the SSU supports this, showing drones striking exactly at pre-identified structural points.

Figure 0.2 Image released by the Security Service of Ukraine showing drones hidden in a false roof of the Trucks (Chapple, 2025)

Highlights

Although there is no official confirmation that the drones carried out AI-assisted autonomous attacks, the use of AI-driven object recognition within their control systems likely enhanced the operators' precision in targeting specific weaknesses in enemy aircraft. Essentially, while the drones were remotely piloted, they may have had the capability to perform final targeting with the help of onboard computational tools. The mission's success was not solely due to advanced technology; it was equally the result of strategic planning, thorough intelligence gathering, and efficient logistics that allowed Ukraine to hit vital components of Russia's strategic air power well beyond the frontlines.

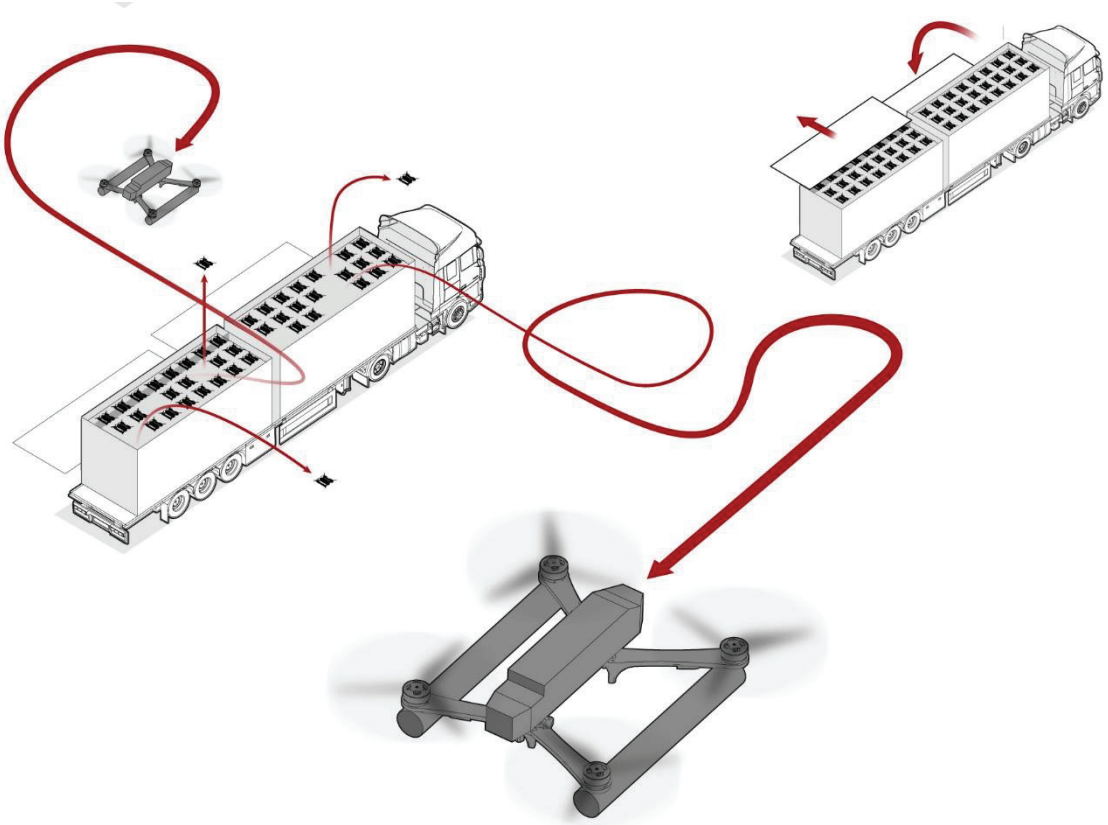

Figure 0.3 Illustration of the Drone Attack (White et al., 2025)

Estimated Cost of Losses

The SSU has estimated the cost of the equipment destroyed as a result of Operation Spider's Web is over US$7 billion. A senior NATO official called the operation the most successful one yet. The Alliance estimated that at least 40 aircraft were damaged and between 10 and 13 aircraft were destroyed.

Relocation of Russian Assets

Russia has relocated dozens of its strategic bombers to more remote airbases across the country in the wake of this month's sweeping Ukrainian drone assault on Moscow's military aircraft, satellite imagery suggests.

Ukrainian security services conducted a massive drone attack against Russian military airbases on June 1, striking thousands of kilometres from the front line in what President Volodymyr Zelensky said was their longest-range operation ever. The attack, named "Operation Spider's Web," targeted multiple airbases deep inside Russia, including in the Murmansk, Irkutsk, Ryazan and Ivanovo regions.

Beyond the battlefield, Operation Spiderweb reshapes strategic assumptions, diplomatic dynamics, and the very nature of deterrence. It reaffirms the principle that innovation and resolve can compensate for size and scale, and it establishes Ukraine as a formidable actor capable of transforming adversity into strategic advantage.

This operation was not just about damage it was about declaring that in the 21st century, even a smaller power can strike at the heart of a larger one, provided it has the ingenuity, the intelligence, and the will. As nations around the world take note, the lessons of Operation Spiderweb may well define the next generation of military and hybrid conflict.

Analysis of the Attack

Operation Spiderweb marks a significant inflection point in the ongoing conflict between Ukraine and Russia. Notable not only for its technical sophistication and daring execution, but the operation also reflects a broader transformation in the nature of contemporary warfare. It exemplifies a decisive shift from conventional, attrition-based combat toward a more intelligent, asymmetric mode of conflict one that effectively leverages civilian and commercially available technologies. Utilizing relatively low-cost assets, Ukraine successfully penetrated and disrupted critical infrastructure deep within the Russian Federation, previously regarded as secure and impenetrable.

The Role of Artificial Intelligence

A central question arising from this operation concerns the factors that enabled an attack of such scale and effectiveness. A key enabler appears to be the integration of artificial intelligence (AI) into Ukraine's drone capabilities. AI-powered unmanned aerial vehicles (UAVs) were deployed from concealed, custom-modified transport vehicles and launched in proximity to high-value Russian air bases. Operating in semi-autonomous swarms, the drones were remotely guided via Russia's own mobile telecommunications infrastructure, which provided sufficient bandwidth to transmit real-time visual data to operators located in Ukraine. Prior to the strike, the drones were equipped with AI-generated intelligence that analyzed structural vulnerabilities of targeted aircraft, thereby enhancing the precision and lethality of the assault (Horowitz, 2025).

Nature and Implications of the Asymmetric Strike

Operation Spiderweb is emblematic of asymmetric warfare, highlighting how even heavily fortified targets remain susceptible to non-traditional threats. While strategic installations are typically designed to repel large-scale assaults, they often remain vulnerable to small, decentralized, and technologically agile incursions. This vulnerability is analogous to the battlefield asymmetry where inexpensive rocket-propelled grenades (RPGs) can neutralize heavily armored tanks. The operation underscores the urgent need for advanced counter-unmanned aircraft systems (CUAS), particularly for the protection of high-value military assets and bases.

The bombers targeted in this operation play a crucial role in Russia's capacity to project force over long distances and deliver payloads deep into adversarial territories. Some of these aircraft

have previously been used to launch ballistic missile strikes within Ukraine. While the full extent of the operational impact remains to be assessed, it is reasonable to conclude that the strike has disrupted not only Russia's long-range strike potential but also its broader surveillance and reconnaissance capabilities.

Strategic Forecast

In light of this event, there is a compelling need for the Russian military establishment to reassess the vulnerabilities of its critical air and naval infrastructure, including bases that host nuclear-capable platforms. Given Ukraine's expanding long-range precision strike capabilities and the limited progress along conventional battlefronts, it is highly probable that similar attacks will be conducted with increased frequency. The Spiderweb operation signals a new phase in the conflict, one where technological innovation and adaptive strategy may outweigh conventional military superiority.

Russian Punitive Strike

Russia launched a massive punitive bombing attack against Kyiv's daring **Spider's web** drone assault. Friday's massive bombing was Putin's biggest attack since Kyiv's daring drone assault took out dozens of strategic bombers at Russian airfields(Bondar, 2025).

- KYIV — Russia launched a huge barrage of missiles and drones against a broad swath of Ukrainian territory early Friday, killing at least three people and injuring more than 40 others that took out dozens of strategic bombers at Russian airfields on June 1.

- In total, over 400 drones and more than 40 missiles including ballistic missiles were used in this attack. Almost all of Ukraine were targeted in this attack Volyn, Lviv, Ternopil, Kyiv, Sumy, Poltava, Khmelnytskyi, Cherkasy, and Chernihiv regions.

- The attack was described as one of the largest since the beginning of the war. Russia also targeted other areas in Ukraine including its largest city, Kharkiv.

- **Ukraine's air force said 452 drones and missiles were launched against the country, with airstrikes recorded in 13 locations, in an attack that lasted more than four hours. More than 400 of the drones and missiles were shot down or otherwise neutralized, the air force said.**

Comments:

- It is pertinent to examine whether Operation Spider Web, a Ukrainian drone attack targeting Russian airbases, was likely a worthwhile strategic and psychological victory for Ukraine, despite the subsequent Russian retaliation.
- **While Russia did respond with increased aerial attacks, the operation inflicted significant damage on Russian military assets, including nuclear-capable bombers, and demonstrated Ukraine's ability to strike deep inside Russian**

territory. This raised the cost of the war for Russia and potentially influenced the calculus of future negotiations.

Significant Damage Operation Spider Web resulted in the destruction or damage of over 40 Russian military aircraft, including strategic bombers, causing an estimated $7 billion in losses. This included the disruption of early warning radar systems.

Strategic Impact The attack targeted Russian airbases far from the front lines, demonstrating that even seemingly secure locations were vulnerable to Ukrainian strikes. This forced Russia to reassess its defensive posture and potentially divert resources to protect its rear areas.

Psychological Effect The operation boosted Ukrainian morale and served as a powerful message that Ukraine could inflict significant damage on Russia, potentially influencing the trajectory of the war.

Retaliation Russia responded with increased aerial attacks on Ukrainian infrastructure and military targets. However, the scale and nature of the Ukrainian attack, particularly its targeting of strategic assets, likely forced Russia to reassess its strategy.

Potential for Diplomacy Some analysts suggested that the attack, while not immediately altering Putin's goals, could push Russia towards diplomacy by demonstrating the cost of continuing the war.

Conclusion

Operation Spider's Web serves as a compelling case study in the evolution of modern warfare, highlighting both Ukraine's tactical innovation and the transformative role of emerging technologies in contemporary conflict. The operation underscores three critical trends that merit urgent attention from military strategists and policymakers worldwide.

First, the proliferation of low-cost, easily replicable technologies—spanning both hardware and software—is accelerating rapidly. Commercially available first-person view (FPV) drones, open-source coding platforms, and artificial intelligence models, initially developed for civilian or recreational use, are now being effectively weaponized. This democratization of military-grade capabilities enables both state and non-state actors to harness disruptive tools with minimal investment. Such developments necessitate proactive regulation, threat anticipation, and the design of countermeasures tailored to this evolving risk environment.

Second, the advancement of autonomous functionality in unmanned systems is reshaping operational paradigms. While current drones often divide responsibilities—such as navigation, targeting, and strike execution—into semi-autonomous modules, future systems are likely to consolidate these functions. The result will be fully autonomous platforms capable of executing complex missions across extended ranges with limited human oversight. This shift will profoundly impact military doctrines, command accountability frameworks, and ethical debates surrounding the delegation of lethal force to machines.

Third, the operation reveals the growing inadequacy of traditional defenses against novel aerial threats. Critical infrastructure—both military and civilian—faces increasing exposure to small, agile, and low-signature drones. These systems frequently evade legacy air defense architectures, necessitating a new generation of protection strategies. Investments in early warning systems, electronic countermeasures, and multi-layered defense networks are becoming indispensable.

Collectively, these trends suggest a redefinition of strategic advantage in modern warfare: one based less on sheer industrial capacity and more on technological adaptability and resilience. Armed forces that prioritize innovation in doctrine, preparedness, and defensive infrastructure will be best equipped to navigate the uncertainties of an increasingly automated and asymmetric battlespace.

References

Bego, K. (2025, June 6). *Ukraine's Operation Spider's Web is a game-changer for modern drone warfare. NATO should pay attention* |. Chatham House. https://www.chathamhouse.org/2025/06/ukraines-operation-spiders-web-game-changer-modern-drone-warfare-nato-should-pay-attention

Bondar, K. (2025, June 2). *How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare*. CSIS. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

Borsari, F. (2025, June 10). *Ukraine Attack: The Spider's Web Still Needs Humans - CEPA*. Center for European Policy Analysis (CEPA). https://cepa.org/article/ukraine-attack-the-spiders-web-still-needs-humans/

Chapple, A. (2025, June 2). *How Ukraine's "Spiderweb" Drone Attacks May Change Modern Warfare*. Radio Free Europe. https://www.rferl.org/a/russia-air-base-drone-attack/33431837.html

Gibson, O., Harvey, A., Novikov, D., Harward, C., & StepanenkoKateryna. (2025, June 1). *Russian Offensive Campaign Assessment, June 1, 2025 | Institute for the Study of War*. Instiute for the Study of War. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-june-1-2025

Horowitz, M. C. (2025, June 3). *Ukraine's Operation Spider's Web Shows Future of Drone Warfare*. Centre for Foreign Relations. https://www.cfr.org/expert-brief/ukraines-operation-spiders-web-shows-future-drone-warfare

Starchak, M. (2025, June 10). *Ukraine's Drone Attack on Russia's Strategic Aviation Has Broader Implications*. Carnegie Endowment for International Peace. https://carnegieendowment.org/russia-eurasia/politika/2025/06/russia-nuclear-force-shuffle?lang=en

White, M. C.-, Dutta, P. K., & Zafra, M. (2025, June 5). *How Ukraine pulled off an audacious drone attack deep inside Russia*. Reuters. https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES-RUSSIA/mypmjzayyvr/

About the Author

Brig Anubir Singh Chahal is a veteran and was commissioned & commanded 16 MARATHA LI bn , during his Comd tenure he got injured and was awarded SM for gallantry. The officer is a graduate of DSSC course and attended the Higher Comd course at the Army War College, Mhow. The officer has tenanted Regt , instructional and Comd appointments during the course of his service including a stint at IMTRAT , Bhutan.